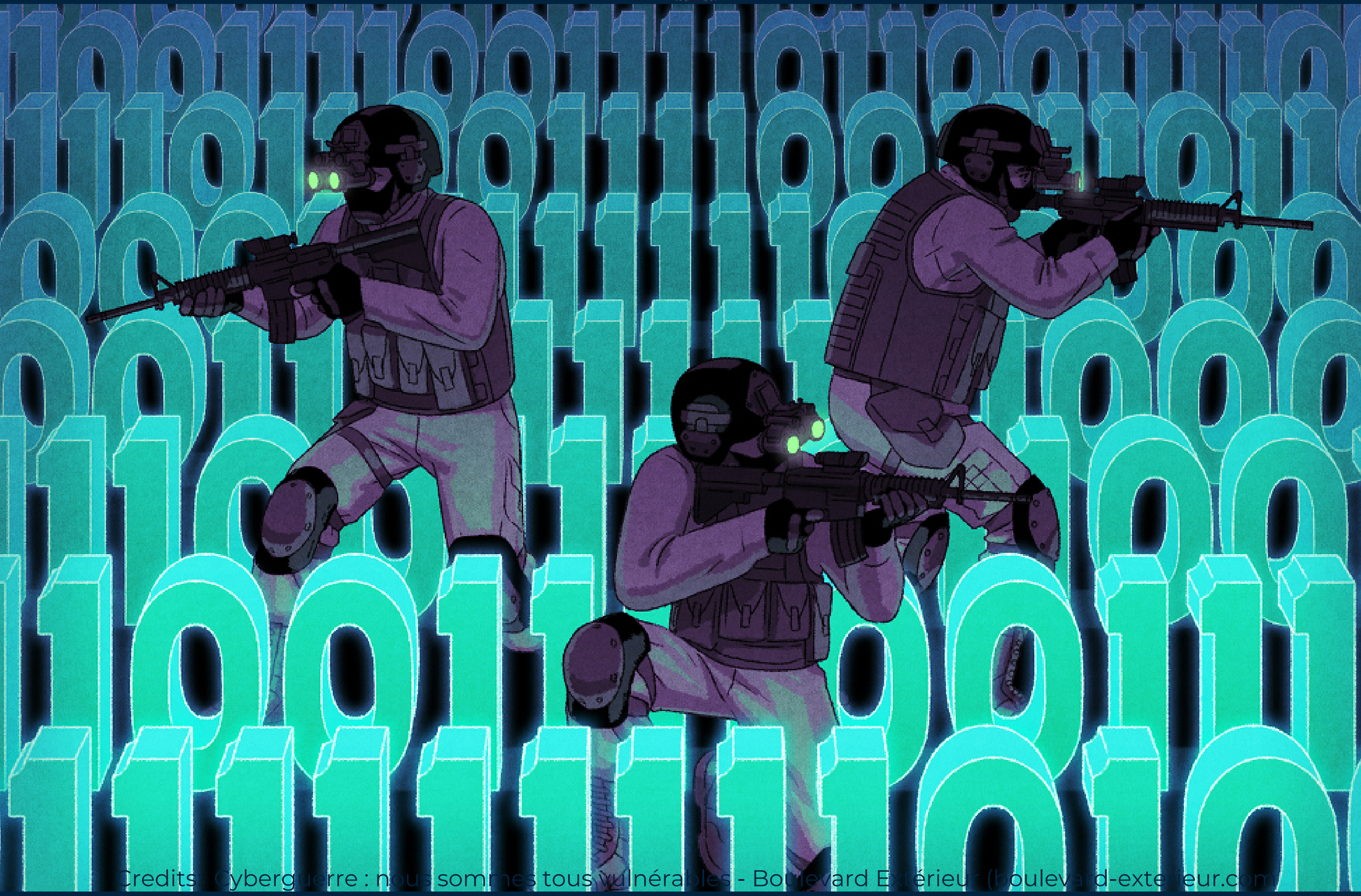
LE COMBAT CYBERNÉTIQUE

ALISÉE MOURA
FÉVRIER 2022



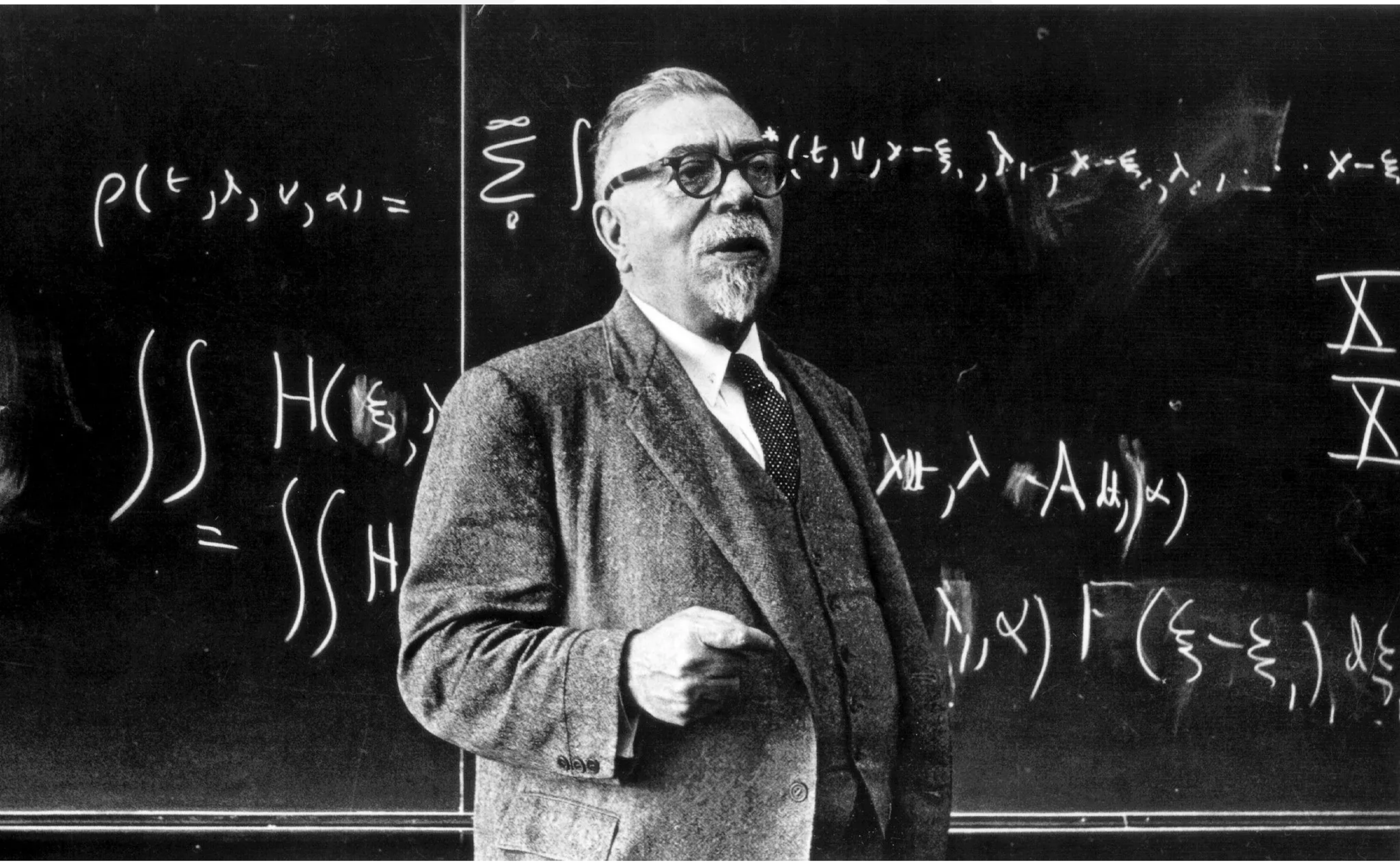
Credits : Cyberguerre : nous sommes tous vulnérables - Boulevard Extérieur (boulevard-exterieur.com)

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65

QU'EST CE QUE LA CYBERNÉTIQUE ?

La société de l'information se caractérise par la diffusion croissante et continue des systèmes d'information dans nos organisations personnelles et professionnelles, qui sont toutes affectées par l'introduction de l'informatique pour créer, stocker, analyser et le cas échéant détruire des données. Nous devons l'apparition du mot "cybernétique" à Norbert Wiener, enseignant au Massachusetts Institute of Technology (MIT) qui dans un livre paru en 1948 établit cette définition de ce terme qui désigne "le champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal". Avec l'instauration et le déploiement du cyberespace, nous sommes entrés concrètement dans l'ère de la "Nouvelle Frontière", telle qu'elle a été décrite par John F. Kennedy le 15 juillet 1960 dans son discours d'acceptation d'investiture à la Convention du Parti démocrate :

"Mais je vous dis que nous sommes devant une Nouvelle Frontière, que nous le voulions ou non. Au-delà de cette frontière, s'étendent les domaines inexplorés de la science et de l'espace, des problèmes non résolus de paix et de guerre, des poches d'ignorance et de préjugés non encore réduites, et les questions laissées sans réponse de la pauvreté et des surplus."



La guerre cybernétique va donc intégrer les usages offensifs et défensifs de ces systèmes d'information dans le cadre de l'affrontement entre les nations. En ciblant les infrastructures militaires mais également les équipements administratifs, économiques, financiers, industriels et sociaux.

Credits : Mais où va le web

EN QUOI SE DIFFÉRENCIE-T-IL D'UN MODE D'ACTION TRADITIONNEL ?

Le Droit International Humanitaire et le Droit des Conflits Armés ont permis d'établir des distinctions dans le traitement qui doit être réservé aux populations civiles lors d'un conflit. Néanmoins, en matière de cyberguerre les cibles non militaires ne bénéficient d'aucun traitement privilégié. En effet, les banques, les entreprises, les hôpitaux, les particuliers, les universités ou les écoles sont visés régulièrement par des cyberattaques. Afin d'amplifier les dysfonctionnements dans le pays ciblé ou pour accroître l'exposition médiatique de l'agression.

La technologie est sans frontière. Il suffit de quelques secondes pour déplacer des fichiers d'un ordinateur à un autre et donc possiblement d'un pays à un autre. En plus, ce n'est pas parce que l'origine d'une attaque informatique a été localisée dans un pays, que l'on peut déterminer avec une certitude absolue cette identification. Il peut s'agir d'un énième rebond technique pour leurrer les pisteurs informatiques. Et cela ne signifie pas que les autorités du pays en question sont nécessairement informées que l'action en question part de leur territoire, ni qu'elles ont donné leur accord pour cela. C'était plus fréquemment le cas lorsqu'on avait affaire à des armées physiques. La localisation n'implique donc pas de facto la responsabilité du pays dans lequel se trouvent les auteurs présumés de l'attaque informatique. Il n'y a pas de lien systématique. Cela est important à prendre en compte dès lors qu'une riposte est envisagée.

Credits : Pixabay

QUELLE RÉPONSE À UNE CYBERATTAQUE ?

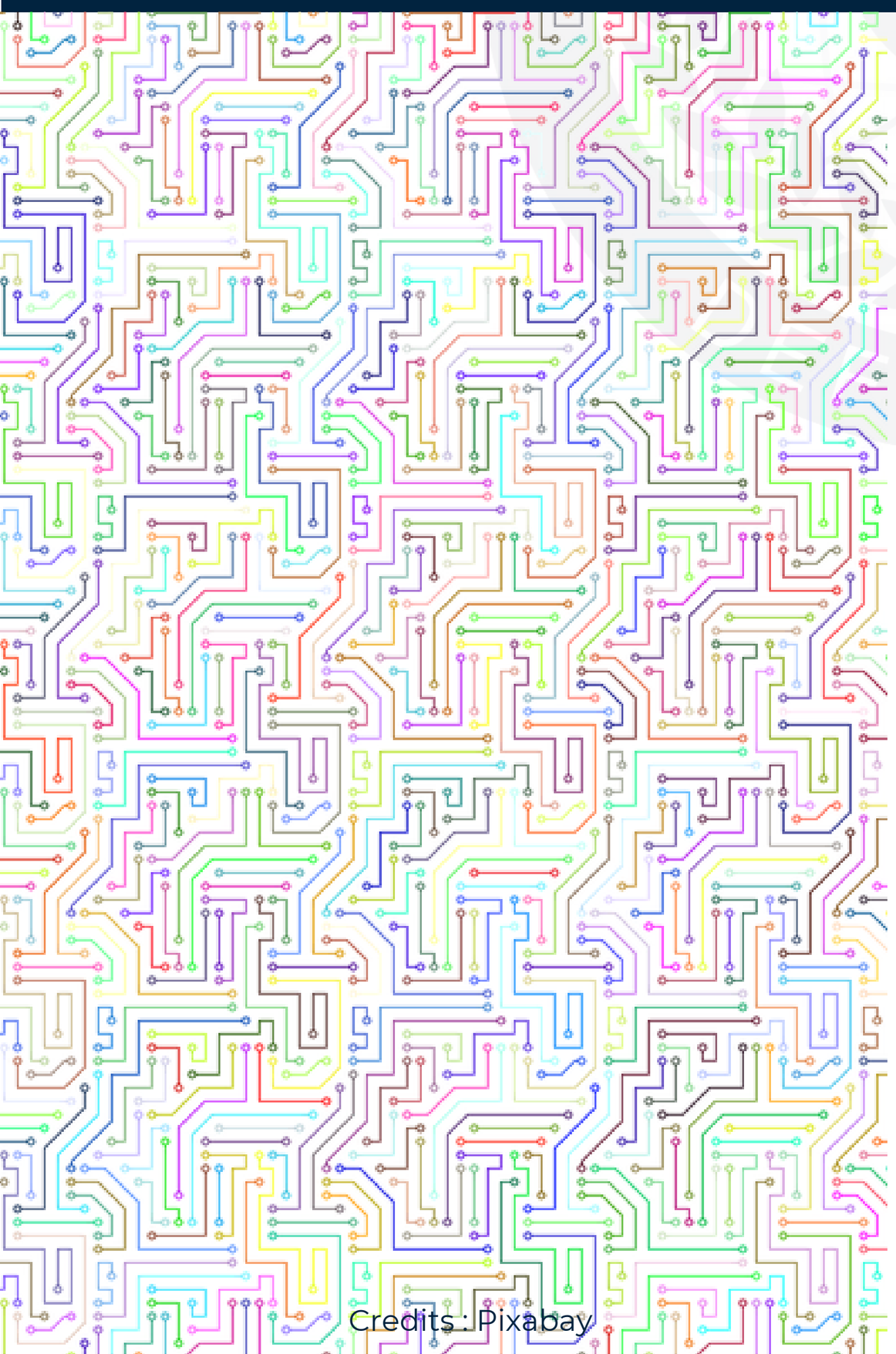
Une fois connue, la cyberattaque peut susciter l'envie de riposter. Mais cela pose quatre questions majeures :

- La proportionnalité : comment doser la riposte ?
- La simultanéité : quand considère-t-on que la cyberattaque est survenue ?
- L 'imputabilité : comment est-on certain d'avoir déterminé les auteurs de l'attaque ?

Dès 2009, des hauts fonctionnaires de la Défense aux Etats-Unis ont estimé qu'une cyberattaque pouvait susciter une réponse militaire conventionnelle. En 2011, Washington a officiellement reconnu qu'une cyberattaque pouvait être assimilée à un acte de guerre.

Credits : Pixabay

L'INCLUSION DE LA CYBERNÉTIQUE : UNE RÉPONSE AU TERRORISME ?



Credits : Pixabay

Le ministère des Armées en France précise que la menace cyber ne se résume plus seulement à des attaques informatiques pouvant détruire ou perturber des systèmes d'informations, elle prend également place dans le domaine informationnel.

Les groupes armés terroristes, au Levant mais aussi en Afrique ou au Maghreb ont investi massivement dans l'espace numérique. Leur but est de terroriser son ennemi pour l'empêcher de combattre, apparaître plus fort qu'on ne l'est en réalité ; recruter à l'aide de campagnes de propagande mensongères mais sophistiquées ; désorganiser en propageant des fausses rumeurs et / ou en les amplifiant sur les réseaux sociaux. Un nouveau terme est dorénavant utilisé pour expliquer ce mode d'action : la "barbarie numérique". Cela constitue une véritable inflexion stratégique avec l'inclusion de l'hybridité du combat dans le cyberespace. Les frappes de drone constituent un mode d'action hybride sans impliquer des combattants, une véritable réponse déshumanisée. La guerre menée par la CIA à l'aide des drones contre les cellules terroristes au Pakistan, en Somalie par exemple, illustre cette guerre furtive.

QUELLE PLACE POUR LE DROIT INTERNATIONAL ?

Il semble que le droit international semble quelque peu démuni face aux accélérations du progrès technologique car il ne prend pas en compte la pluralité des nouveaux acteurs et la résurgence de nouvelles menaces s'inscrivant dans cette dimension immatérielle qu'est le cyberespace.

En effet, comme le souligne le chapitre 7 de la charte des Nations Unies, le cadre de la légitime défense (article 51) ne s'applique qu'à l'égard d'un Etat.

On constate une véritable inadéquation dans la marche à suivre et quelle attitude adopter.

On peut donc se questionner sur la nécessité de repenser le droit international, sachant que les résolutions du Conseil de Sécurité ne sont pas nécessairement en concordance avec la Charte des Nations Unies notamment au sujet de la lutte contre le terrorisme.

Ainsi, la nature "d'exception" prend tout son sens avec la résolution 2249 autorisant l'intervention contre Daech, puisqu'elle montre son lot d'ambiguïté entre intervention préventive et véracité de la légitimité.

Avec l'usage de plus en plus fréquent du lawfare ou "guerre par le droit", une inquiétude plane envers et contre les silences de la loi pouvant permettre à des criminels d'agir en toute impunité.

Cette impunité imputée à la cybersphère paraît effrayante car si le droit ne définit pas déjà précisément une jurisprudence définie, comment peut-on stopper la cybercriminalité ?

Crédits: L'emblème et le drapeau de l'ONU | Nations Unies
Daech aurait divisé par deux le salaire de ses combattants | Konbini

LE DROIT INTERNATIONAL : UN ABONNÉ ABSENT ?

Il n'existe qu'un seul texte de dimension internationale dans le cyberespace : la Convention de Budapest de novembre 2011 relative à la cybercriminalité. Malgré les tentatives diplomatiques dans le cadre des Sommets mondiaux sur la Société de l'Information (SMSI) organisés par l'Union International des Télécommunications en 2003 à Genève et en 2005 à Tunis. Depuis lors, ces réunions internationales n'ont abouti à rien de concret. Interpol, Europol et Eurojust s'organisent pour faciliter la coopération policière et judiciaire. Mais leurs procédures et leurs moyens techniques ou juridiques sont encore très loin de pouvoir rivaliser avec l'hyperréactivité de l'informatique, ainsi qu' avec la créativité des attaquants.

Crédits: Marija Pejčinović Burić : La Convention de Budapest reste la norme internationale la plus adaptée à la répression de la cybercriminalité - Cybercrime@Octopus: News (coe.int)

LA PRÉVENTION DU COMBAT CYBERNÉTIQUE A LA CHARGE DES ETATS

Après les révélations du consultant Edward Snowden en 2013 et de nombreuses cyberattaques ayant visé des gouvernements et des multinationales, la situation évolue peu. En septembre 2015, Pékin et Washington ont entrepris d'établir un pacte de non-agression dans le cyberespace. Mais sans que le détail de ses critères d'application ni les sanctions encourues en cas de non-respect de celui-ci soient connus. Loin d'une discussion multilatérale, on semble s'orienter vers des négociations bilatérales entre puissances qui savent chacune ce qu'elles ont à craindre de l'autre.

Crédits: Washington et Pékin négocient un accord de non-agression dans le cyberespace (lemonde.fr)

SOURCES

- Djerbi, Samir Ouali. « Vers le combat cybernétique », Revue Défense Nationale, vol94, no. 9, 2016, pp. 121-126.

- Coustillière, Arnaud. « Cyberdéfense militaire : placer le combat numérique au cœur des opérations », Revue Défense Nationale, vol. 784, no. 9, 2015, pp. 11-14.

- Clech, Jérôme. « L'hybridité : nouvelles menaces, inflexion stratégique ? », Revue Défense Nationale, vol. 788, no. 3, 2016, pp. 12-18.

H.E.I.P

AEROSPACE
CYBERSECURITY

DEF'INSEEC

SUIVEZ DEF'INSEEC SUR

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65